CLOUD COMPUTING SECURITY ISSUES AND ITS CHALLENGES

Abu Salim and Rajesh Kumar Tiwari

ABSTRACT

Cloud computing represents a transformative approach to computing, enabling the sharing of resources like hardware, networks, and storage on remote servers via the internet. It facilitates the delivery of applications, computing power, and infrastructure to users as a service. This model provides users with a cost-effective Information Technology (IT) solution, as it allows the dynamic scaling of resources based on demand. In this paradigm, Cloud Service Providers (CSPs) handle all computing needs, offering flexibility and scalability. However, the cloud's reliance on remotely located servers introduces several challenges, particularly from a user's perspective. Both the data and applications are stored on servers that may reside outside the user's geographical or legal jurisdiction. This decentralized storage and processing model raise critical concerns about data security, privacy, accessibility, and compliance with regional laws. These issues often act as significant barriers to the broader adoption of cloud computing technologies.

This article aims to examine the key challenges associated with cloud computing that hinder its broader adoption.

Index Terms *Cloud Computing, Security concern, Key Characteristics, key Challenges, Delivery Model.*

Reference to this paper should be made as follows:

Abu Salim and Rajesh Kumar Tiwari. ***'****CLOUD COMPUTING SECURITY ISSUES AND ITS CHALLENGES, Int. J. of Electronics Engineering and Applications, 8, Issue II, July-Dec 2020, pp 69-81, DOI- 10.30696/IJEEA.VIII.II.2020.69-81.*

Biographical notes:

Abu Salim completed B.Tech and M.Tech in Computer Science and Engineering. He is currently pursuing Ph.D. from the Glocal School of Technology and Computer Science, Glocal University, Saharanpur. His research interests include cloud computing, data security, and machine learning.

Rajesh Kumar Tiwari holds MTech and Ph.D. in Computer Science. He is currently working as an Associate Professor at the Glocal School of Technology and Computer Science, Glocal University, Saharanpur. His research focuses on data security, network security, cloud computing, and database management systems**.**

I. INTRODUCTION

Cloud computing is the outcome of extensive study being conducted by academics in academia and industry with the goal of developing superior technology. As a consequence of their efforts, cloud computing has been developed.

Distributed computing may take several forms, including the grid and cloud computing, both of which are based on the service provisioning concept. Users make a payment to the service provider in exchange for utilizing the service. One definition of a distributed computer system is one in which the various software components are located on system. It is comparable to the traditional networks of individual computers that are used to solve complex issues by delegating tiny pieces of the issue to a large number of computers and then merging the answers generated by those computers.

Using grid computing, you are able to treat computer resources like a utility that can be switched on or off at any time. The delivery of resources on demand is a further advancement made possible by cloud computing. It does away with the need of the practice of providing more than is necessary in order to satisfy the requirements of a large number of consumers.

The term "cloud computing" refers to a model in which computing is delivered more as a service than as a product. With this model, shared resources such as hardware and software are made available to personal computers and other devices (tablets, mobile phones, etc.) as a utility across a network.

It makes use of self-service, pay-as-you-go, high-availability, high-performance, and scalable computing services that are delivered through the internet. These services are available on a pay-per-use basis. There is a vast selection of services accessible today, ranging from basic infrastructure hosting (also known as IaaS) to complete development platform hosting (also known as PaaS), and applications hosting (also known as SaaS).

Cloud computing may shorten the amount of time it takes to bring a product to market since a new server can be set up or brought online in a hurry. Users are able to avoid making expensive initial capital expenditures in the infrastructure thanks to this. Enhance the adaptability of the company as well as the IT organization, which enables companies to pay for extra capacity only when it is really required by the business.

Cloud computing, like many other wonderful prospects, also provides a large number of obstacles and hazards [1,2] all of which IT personnel and decision makers need to be aware of.

A. Characteristics of Cloud Computing

The cloud computing paradigm utilizes three delivery models and four deployment models, has five important qualities, and has critical properties.

Key features include:

Ubiquitous Network Access enables users to access applications and data via a variety of various types of devices, including mobile phones, tablets, and personal computers.

On demand self-service, customers have access to and control over their own computer resources on demand, which is known as “on demand self-service”.

Rapid elasticity, the user is able to acquire or release resources in a fast and automated manner

according to their needs.

Measured Service, the user's usage of the cloud's resources may be monitored, and the user will be paid based on the resources that they really put to use.

Pooling Available Resources, a CSP may make their resources (hardware and software) available to many users. The user is able to either acquire or release resources depending on their needs.

B. The Delivery of Cloud Computing Services

Cloud computing makes use of three main delivery models, each of which facilitates the delivery of a certain category of service to the end user. The software as a service (SaaS), the platform as a service (PaaS), and the infrastructure as a service (IaaS) delivery models are the models that supply the user with infrastructure resources, application platforms, and software respectively. Additionally, each of these service models imposes a unique degree of security need on the underlying cloud infrastructure.

Software as a Service (SaaS): Software as a Service, often known as SaaS, is a software deployment paradigm in which applications are remotely installed on a server by the CSP, and cloud customers are then able to access the services that have been installed on the server. SaaS provides customers of cloud computing with a variety of advantages, including a reduction in both the initial investment and the ongoing costs of operation. However, the majority of corporations are still hesitant because of a variety of concerns, including trust, privacy, and security. Companies like Salesforce are examples of companies that provide PaaS. Salesforce provides cloud-based CRM software as a service product on the market. Another well-known SaaS product is Google's email service, Gmail.

Infrastructure as a Service (IaaS): Infrastructure as a Service, often known as IaaS, is a model that totally alters the application deployment process for developers. They can simply go to one of the IaaS providers, have a virtual server operating in a matter of minutes, and pay only for the resources that they use as opposed to investing a significant amount of money on their own data centers. IaaS and other linked services have, in a nutshell, made it possible for start-ups and other enterprises to concentrate on their primary areas of expertise without being distracted by concerns over their IT infrastructure. IaaS only offers the most fundamental level of security; applications migrating into the cloud will demand greater degrees of security and will need to comply with regulatory standards. Amazon Web Services, GoGrid, and Rackspace are a few examples of companies that provide IaaS.

Platform as a Service (PaaS): PaaS is one layer above IaaS on the stack, and it abstracts everything up to and including the operating system, middleware, and other software. This provides a unified environment for software developers, which includes, developer may use to construct their apps without having any knowledge about what is happening underlying the service they are using. It provides developers with a service that manages the whole software development life cycle, from planning to designing to creating applications to deploying to testing to maintaining software. The developers don't have a "view" on anything else since it has been abstracted away. The disadvantage of PaaS is that its benefits may make it easier for hackers to use the PaaS cloud infrastructure as a command-and-control center for malware and to circumvent IaaS applications. This is the "dark side" of PaaS. PaaS services include force.com, Google App Engine, and Microsoft Azure, as few examples.

C. Models for the Deployment of Cloud Computing Services

There are four different deployment models that are used by cloud computing.
Public Cloud is a sort of cloud computing in which the cloud infrastructure is controlled by an organization that sells cloud services and is made accessible to the general public or to a big industry group.

Community cloud refers to a specific kind of cloud computing in which the cloud infrastructure is used by a number of different organizations that have similar concerns (for example, mission, security).

Private Cloud, a private cloud is a kind of cloud computing in which the cloud infrastructure is used by a single business that may be physically situated on or away from the company's premises.

Hybrid Cloud is a type of cloud computing that consists of two or more clouds (private, community, or public) that continue to exist as separate entities but are connected through the use of standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load-balancing between clouds).

D. Users and Providers of Cloud Services

Cloud computing involves participation from a variety of parties, including cloud users, cloud providers, cloud resellers, and cloud service brokers.

Cloud Providers: Internet service providers, telecommunications firms, and big business process outsourcers are examples of the types of organizations that fall under the term "cloud providers." These companies either supply the infrastructure (hosted data centers) or the media (Internet connections) that allow customers to access cloud services. In addition, system integrators might be considered service providers. These companies construct and maintain data centers and provides a variety of services (such as SaaS, PaaS, IaaS, and so on) to end users, service brokers, and resellers.

Cloud Service Brokers: Cloud Service Brokers are comprised of individuals and organizations such as technology consultants, business professional service companies, licensed brokers and agents, and influencers that assist customers in making decisions about cloud computing solutions. Without really owning or controlling the whole Cloud infrastructure, service brokers focus on the negotiation of the agreements that exist between customers and suppliers of cloud services.

Cloud Resellers: Cloud resellers are local businesses who have been selected by a CSP in order to expand that provider's customer base. They provide the impression of being a cloud provider in a certain location, but in reality, they are supplying services with the assistance of another Service Provider.

Cloud Users: Cloud Users are at the very bottom of this chain since they are the ones who really utilize the services that are provided by CSP.

2. RESEARCH METHODOLOGY

In this study, we have employed both forward and backward search method. In order to collect information, we have searched research papers, internet sources and journals. The articles are searched on the websites such as: IEEE-Xplore, the ACM digital library, Google Scholar, Elsevier. Throughout the course of our investigation, we made use of several keywords such as "cloud computing security," "cloud computing security challenges," and "top cloud security issues", which were located in the titles, abstracts, or keywords of various papers. After careful consideration, certain references were excluded because they were unusable like the quality of the paper, duplicated information presented, contained less information. After observing around 100 publication the following security issues are identified.

3. MAJOR OBSTICLES IN CLOUD COMPUTING

In this section, we will explore the key challenges identified through a systematic review that cloud computing must address. These challenges play a key role in shaping the growth, adoption, and efficient utilization of cloud-based technologies. A detailed examination of these obstacles provides valuable insights into the barriers challenging the cloud computing.

Unauthorized Access:
Contrary the company's on-premises architecture, cloud-based installations are accessible directly from the public Internet and are located outside of the company boundary. Because of this, users and customer will find the infrastructure to be more accessible. However, attackers are also given an easier time, gaining unauthorized access to a company's cloud-based services. If security is set incorrectly or credentials are stolen, an attacker may be able to bypass the company's protections and get direct access to the system without the company awareness.

Insufficient Visibility:
The cloud-based resources of an organization are kept at a physical location that is remote from the corporate network and are operated using hardware that the organization does not own. As a consequence of this, many of the conventional tools that are used to get network visibility do not perform well in cloud settings, and some organizations do not have cloud-focused security solutions. This may make it more difficult for an organization to manage the cloud-based services they use and safeguard those resources from being attacked.

Unintentional Disclosure of Credentials:
Phishers often make use of cloud apps and platforms as a pretext in the assaults that they launch against their victims. People have become familiar to getting emails with links that may ask them to verify their login information before gaining access to a specific document or web page.

Data Privacy:
The capacity of an individual or organization to conceal themselves or information about themselves and reveal themselves only when they want to do so is known as data privacy [3].
In cloud computing, protecting the privacy of one's data is another important consideration. It is necessary for businesses to organize teams of staff members to investigate customers' concerns about data protection. The Information Technology Act, 2000 (often known as the "IT Act") and its several

sub sections control the data security and privacy related concerns in India. It is possible for data stored in the cloud to be dispersed across geographical borders, which may not be following the privacy laws of the area in question.
Information that is held in the cloud is subject to the legal requirements of one or more legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), the cloud provider is legally obligated to preserve the data's privacy in an acceptable way.

Data Security:
When it comes to cloud computing, one of the most important concerns is the safety of the data that is kept at the CSP. In conventional case, the client owns the computer on which the data are kept, so that it is on their property. The client is responsible for providing both the physical and logical security measures. On the other hands, in cloud the user does not have control over the data storage. As the data are stored on a shared environment, the data must be protected by the SaaS provider at all times. They are required to apply a rigorous encryption method and provide fine-grained access control to the data. Once the data has been erased by the user, the SaaS provider should not be able to recover access to it by utilizing any means. The customer should have control over the data life cycle.
whatsoever means. Before data is stored, it is possible for it to be encrypted automatically. The encryption that is offered by hard disk manufacturers has a less impact on the performance overhead. The following test may be used in order to determine whether or not the data kept at the CSP is secure [4].

- [XSS] stands for "cross-site scripting."
- Flaws in the access control system
- OS and SQL injection vulnerabilities.
- Forgery of cross-site requests, often known as CSRF.

Data integrity:
Integrity in data, software, and hardware indicates that assets can only be changed by authorized persons or in permitted way. The term "data integrity" refers to the process of defending data against illegal changes, deletions, or fabrications [5].
In a typical system, ensuring the integrity of the data is not difficult. The integrity of the data is preserved in a system like this one via the use of database constraints and transactions. For the sake of preserving the integrity of the data, transactions need to adhere to the ACID (atomicity, consistency, isolation, and durability) criteria. ACID features, which maintain the database's integrity, are supported by the majority of the database system software, such as Oracle and SQL.
The information that is produced by cloud computing services is stored in the cloud. Users run the risk of losing control of their data when they store it in the cloud and must instead depend on cloud operators to ensure the data's access control and integrity.

Data Lock in:
If a company chooses a platform offered by a CSP that is based on proprietary file formats, then the company runs the risk of being locked into a position known as data lock-in. This scenario makes it far more difficult for the company to switch service providers at some time in the future. Changing CSP is essential in the event that a current cloud provider modifies the terms of service they provide or has service outages that force to look for other options.

As CSPs attract consumers at a quick rate, there has been a rise in the amount of attention paid to the issue of lock-in. The European Network and Information Security Agency (ENISA) identified lock-in as one of the most significant hazards associated with cloud computing in a study that was published in November 2009 titled as “Cloud Security Risk Assessment”. According to the research, “there is currently very little that can be offered in the way of tools, procedures, standard data formats, or service interfaces that could guarantee data and service portability”. Because of this, it could be very difficult for the consumer to go from one provider to another or back to an environment located inside the company itself.

The issue of data lock-in may be solved with the assistance of SNIA's Cloud Data Management Interface (CDMI), which was created by the Storage Networking Industry Association (SNIA). The Cloud Data Management Initiative (CDMI) is the first open standard for cloud computing to be produced by the industry. CDMI offers the capability to control service levels that data gets when it is stored in the cloud as well as a single interoperable data exchange format for securely transporting data and its associated data needs from cloud to cloud [6].

Data Location:

The location of data is a critical factor to consider when working with cloud computing. CSP maintain data centers across the globe, and the differing data privacy laws in various countries can raise concerns. The geographic distribution of these data centers may pose challenges, especially for sensitive information that must remain within national borders. Furthermore, during investigations, accessing specific data may become problematic due to jurisdictional restrictions and privacy regulations [7].

Data Availability:

The term "availability" refers to a system's ability to allow authorized entities to access and utilize it at any time. Ensuring data availability is a major concern for organizations. When data is stored on remote systems managed by third-party providers, there is a risk of system failures caused by the service provider. Since the data relies on a single provider, it becomes inaccessible if the cloud service experiences downtime.

CSPs are responsible for delivering uninterrupted service to their customers 24/7. To achieve this, improvements may be necessary at both hardware and software levels. A multi-tier architectural design should be adopted, utilizing a load-balanced farm of application instances running on a scalable number of servers. Resilience to hardware or software failures, as well as protection against denial-of-service attacks, must be built into the application architecture.

Additionally, organizations must implement a robust business continuity (BC) and disaster recovery (DR) plan to prepare for unexpected events and ensure minimal disruption.

Data Segregation:

Data Segregation refers to the process of separating data to ensure that each cloud client can access only their information without impacting the data of other clients. It is crucial to verify that your CSP implements encryption during data segregation or aggregation and to have security experts review the encryption methods used.

Multi-tenancy is a core feature of cloud computing that allows multiple users to share the same resources, such as hardware and software, simultaneously. This architecture enables multiple clients’ data to coexist within the same physical infrastructure. However, it also increases the risk of intrusion. Such breaches can occur in two primary ways: exploiting security vulnerabilities in the

application and injecting malicious client code into the Software as a Service (SaaS) platform. In the latter scenario, a client could create masked code and inject it into the application. If the application executes this code without proper validation, it could lead to unauthorized access to other users' data. To mitigate these risks, the CSP must establish clear and robust barriers between users' data. Data security should not be limited to the physical infrastructure; it must extend to the application level. The system must possess adequate intelligence and mechanisms to securely segregate data across users, ensuring protection against potential intrusions.

Security Policy and compliance:

A security policy should be comprehensive enough to protect both individuals and information while clearly defining the expected behavior of all entities, including users, system administrators, management, and security personnel. The policy must establish and authorize penalties for violations, articulate the organization's baseline stance on security, aid in reducing risks, and support compliance monitoring with relevant rules and regulations.

When creating a policy to secure data transmission between a cloud hosting provider and a client, several critical factors must be addressed, such as mitigating internal threats and configuring access controls effectively [9]. Security auditing and certification are essential for traditional service providers, and CSPs must also meet these standards to build trust with their clients.

Security audits should comply with industry requirements and standards, such as PCI, HIPAA, and GLBA, while adhering to auditing frameworks like ISO and SAS70. Organizations face significant pressure to ensure compliance with these security standards across all servers, regardless of whether they are hosted on-premises or at remote locations.

Multitenancy:

Cloud computing is characterized by several key features, with multitenancy being one of the most significant. This property allows multiple users to run software on shared hardware resources, optimizing resource utilization. However, despite its benefits [10], multitenancy introduces security and privacy risks.

Virtualization technology is used to isolate cloud customers from one another, but vulnerabilities in applications may allow unauthorized access to another customer’s data, network traffic, or processes. In cloud environments, virtualized application instances are frequently provisioned, allocated, or migrated across multiple physical machines, either on-premises or off-premises, for resource management. This dynamic provisioning increases the complexity of maintaining security, as attackers may exploit shared resources such as hard disks, RAM, or CPU caches.

To address these challenges, the Cloud Security Alliance has proposed several solutions, including conducting regular vulnerability assessments and patches, enforcing strong authentication, monitoring for unauthorized activity, and following best practices for secure installation and configuration. These represent just a few of the eight recommended approaches.

Resolving the challenges of multitenancy, security, and privacy—key obstacles in public cloud adoption—is critical to ensuring the widespread acceptance of cloud computing.

Non-Repudiation:

This term refers to the standards required to prevent any party involved in a cloud interaction from denying that the interaction occurred. Digital signatures play a crucial role in establishing accountability by clarifying roles and responsibilities within an engagement. As described in [11], a tracking method is employed to identify users and determine their origin, making it highly

challenging for users to falsify their identity information while enabling the secure storage of user-related data. The Multi-party Non-Repudiation (MPNR) protocol [12] enhances security by not only safeguarding against rollback attacks but also providing a fair and reliable non-repudiation storage cloud.

Energy Management:

Cloud infrastructure should minimize power consumption while remaining environmentally friendly. Studies reveal that powering and cooling data centers account for 53% of total operating costs [13]. Reducing energy usage not only lowers costs but also benefits the environment.

CSPs are increasingly focusing on energy-efficient data center practices. Efforts include implementing energy-efficient hardware designs that allow CPUs to operate at reduced speeds and shutting down certain hardware components when not in use[14]. Additionally, powering down idle computers is another effective strategy to decrease energy consumption. Techniques such as energy-aware work scheduling and server consolidation further contribute to energy efficiency [15].

Current research aims not only to reduce energy requirements but also to enhance application performance, ensuring a balance between efficiency and effectiveness.

Governance and regulatory compliance:

CSPs are not only responsible for providing Infrastructure and their maintenance, but they also have to incorporate and follow the rules and regulations that are specific to a region's government, such as SOX, HIPAA, FISMA, FIPS 140-2, GLBA, ITAR, ISAE 3402, and SAS 70. In addition, CSPs are responsible for governance and regulatory compliance.

Policies pertaining to governance and regulation that are important are

- Sarbanes and Oxley (SOX)
- The Health Insurance Portability and Accountability Act (often known as HIPAA) ,1996.
- The Federal Information Security Management Act, 2002, or FISMA.
- The Federal Information Processing Standard (FIPS) Publication 140-2, "FIPS 140-2."
- The Gramm-Leach-Bliley Act, abbreviated as GLBA.
- ITAR stands for the International Treaty on the Regulation of Arms.
- INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3402.
- The Statement on Auditing Standards, (SAS70)

Insecure API:

Cloud computing companies often provide clients with a set of software interfaces, commonly referred to as APIs. These APIs serve as comprehensive structural documents that enable customers to manage and interact with cloud services. Key operations such as provisioning, administration, orchestration, and monitoring of cloud resources are carried out through these APIs.

Since APIs are publicly accessible, they may present vulnerabilities that malicious actors could exploit to compromise the security of cloud infrastructure. CSPs share their API specifications publicly for two primary reasons: to inform customers that the services are available and to facilitate architectural adjustments, allowing clients to optimize their use of these services.

Given their public availability, APIs must be carefully designed to ensure secure and seamless functionality for both legitimate and malicious users. Providers must exercise caution in determining

the extent of information shared about system features, ensuring a balance between usability and security.

Service level agreement:

A service level agreement, often known as a SLA, is a contract that discusses the level of services that are anticipated to be given by the cloud provider to the cloud user. It identifies attributes, priorities and obligations. In most cases, it also outlines the corrective actions that will be performed in the event that the service falls below the level that was specified in the SLA. Users of the cloud may choose to form a committee in order to work out SLA. It should fulfill customers' requirements while being cost efficient, and users of the cloud should explicitly identify their demands before signing any contracts. This is obviously a very significant legal agreement between a CSP and a cloud user, and it should include the following [16].

- Determine which services are needed by the user and define them.
- Determine the necessary levels of security and privacy.
- Determine the most important aspects of the services.
- Determine who is responsible for what in the cloud, both users and providers.
- Reduce the conflict.
- A crystal-clear articulation of each party's duties and expectations of the other.
- Determine whether legal and regulatory requirements are met or not.

Trustworthy Service Metering:

CSPs make use of a variety of characteristics in order to bill their customers in accordance with the quantity of services that they have used. For instance, customers are charged by Amazon Elastic Compute Cloud (EC2) based on the amount of time that their particular EC2 instances are in a running state, on the other hand, Google AppEngine users are charged according to the number of CPU cycles that their applications utilize. In cloud computing, multiple users share different resources that are not perfectly isolated and software bugs or intruders may use the services and there uses charges has to be paid by users. This is because users may have little or no visibility into the cloud infrastructure. However, because users may have little or no visibility into the cloud infrastructure, they are often unable to directly connect their actual cloud resource consumption and the usage charges. For the cloud computing paradigm to be successful, figuring out how to assure the reliability of the services being provided is of the utmost importance.

In addition to the issues listed above, cloud computing comes with a number of additional drawbacks, including outages, restrictions on data transmission, slow support response times, increased latency, limited control, a lack of understanding, and challenges in connecting various devices.

- Even the most reliable CSPs might have outages and downtime at some point, even user's own internet connection could also be the source of the issue.
- The ability to send a big volume of data could provide certain difficulties.
- If there is a delay in providing answers to queries raised by customers, customers may have problems.
- latency is the amount of time that passes between when your computer attempts to interface with a server and when it actually does so. It's possible that this will become an issue if interaction is really sluggish.

- Users have limited control over the operation and execution of the hardware and software since the services operate on distant servers. This means that even cloud software may give less functionality than locally accessible software.
- The user may encounter difficulties due to the limited accessibility of information on the operation of cloud servers.
- Users may have difficulties while attempting to integrate several pieces of technology, such as printers, mobile devices, and portable storage units.

4. ANALYSIS OF SECURITY ISSUES

On the basis of systematic review Figure 1 depicts the findings of literature survey of 100 publications on the topics related to security of cloud computing. Location of data, data segregation and service level agreements are the top concern. Unintentional disclosure of data, data loc-in and unauthorized access or other issues that are of the concern.

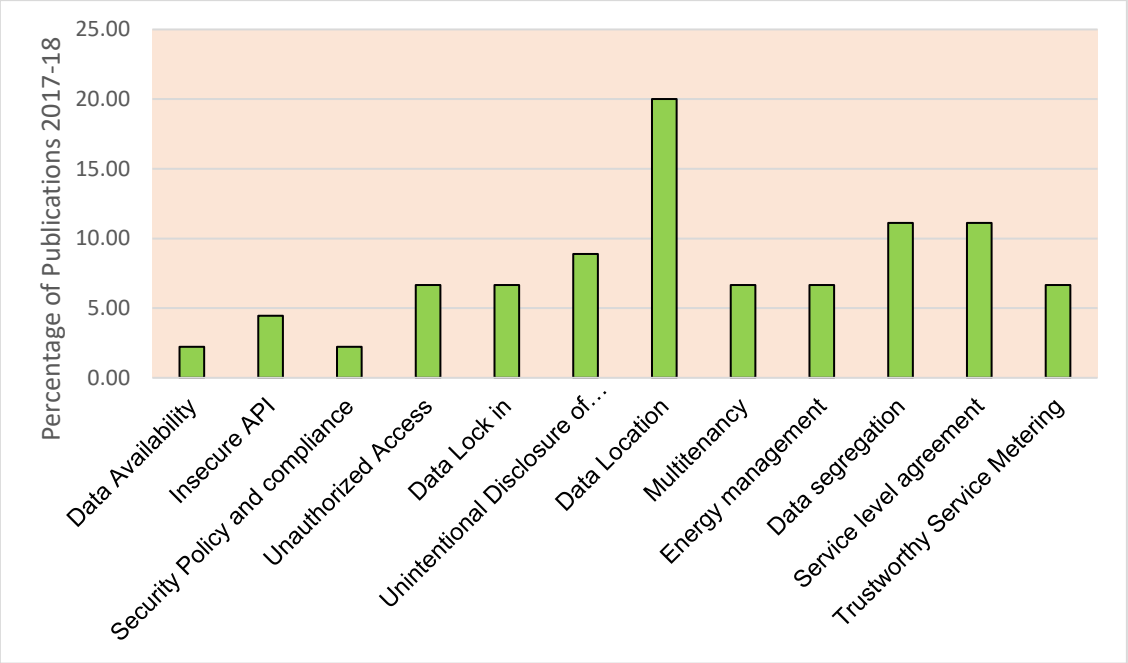

Fig. 1. Percentage of publication on security concern (2017-18) in cloud computing

There are numerous advantages offered by cloud computing as compared to in house services, on the basis of literature survey on the publication citation, the benefits offered by the cloud computing are depicted in the figure 2. We have considered criterion for the inclusion or exclusion of the publication as mentioned in the research methodology. According to our study on demand service, cost effectiveness, resource management ubiquitous access, efficiency is the on the top.

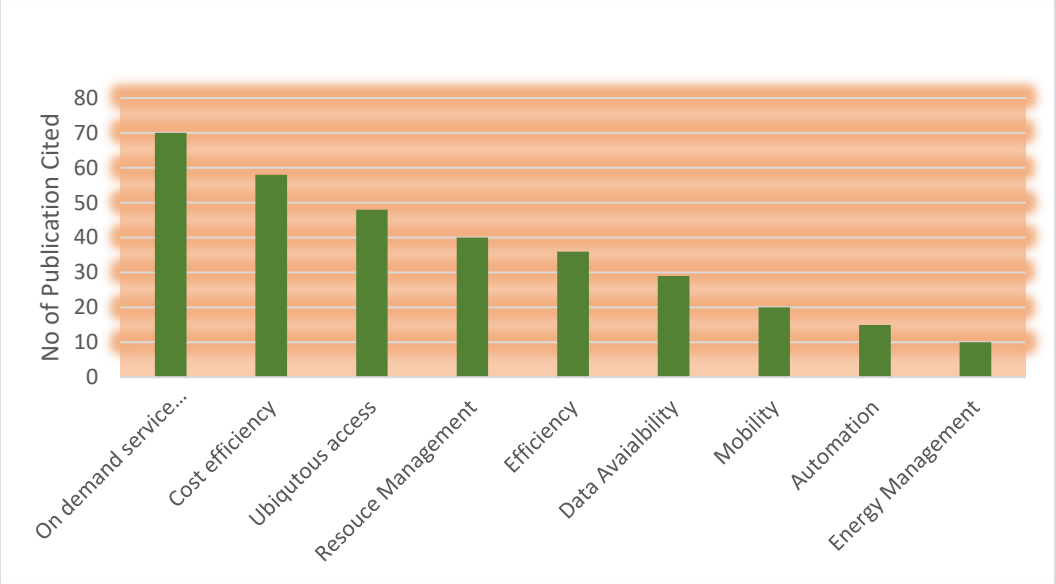

Fig. 2. Publication cited the important features

5. CONCLUSION AND FUTURE WORK

Cloud computing enables the execution of applications and storage of data in remote locations using virtualized computing resources. While this paradigm offers numerous benefits, it also introduces significant challenges related to trust, privacy, and security.

In this study, we have conducted extensive research to identify and analyze the security issues and challenges inherent to cloud computing. Our focus has been on ensuring data security during transmission and storage at the CSP's end. The confidentiality, integrity, and availability of data can be compromised in the multitenant environment of cloud storage, additionally, access control and availability remain critical concerns. Cloud storage providers must implement robust access control mechanisms to ensure that only authorized users can access data, as defined by the permissions granted by the data owner. To guarantee data availability, auditing by a trusted third-party auditor or the data owner is essential.

Future work may include prioritizing the development of a comprehensive security framework to address the key issues like, data security, privacy, integrity, trust management, multi-tenancy, non-repudiation, secure APIs, data lock-in, energy management, Service Level Agreements (SLAs), reliable service metering.

Addressing these challenges will help enhance the reliability, efficiency, and trustworthiness of cloud computing systems, paving the way for broader adoption and innovation in this domain.

REFERENCES

[1] R. Velumadhava Rao and K. Selvamani, (2015), "Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, Vol. 48, pp. 204–209.

[2] M. Rajesh, (2017), "A systematic review of cloud security challenges in higher education," *The Online Journal of Distance Education and e-Learning*, Vol. 5, No. 4, Oct.

[3] D. Suna, G. Changb, L. Suna, and X. Wanga, (2011), "Surveying and analyzing security, privacy, and trust issues in cloud computing environments," *Elsevier*, pp. 2852–2856.

[4] S. Subashini and V. Kavitha, (2011), "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp. 1–11, Jan.

[5] D. Zissis and D. Lekkas, (2012), "Addressing cloud computing security issues," *Future Generation Computer Systems*, Vol. 28, No. 3, pp. 583–592.

[6] SNIA, (n.d.), "The danger of cloud lock-in," [Online]. Available: http://www.snia.org.au/assets/documents/the_danger_of_cloud_lockin_cs.pdf.

[7] R. P. Padhy, M. R. Patra, and S. C. Satapathy, (2011), "Cloud computing: Security issues and research challenges," *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, Vol. 1, No. 2, pp. 136–146, Dec.

[8] K. Ren, C. Wang, and Q. Wang, (2012), "Security challenges for the public cloud," *IEEE Internet Computing*, Vol. 16, No. 1, pp. 69–73, Jan.–Feb.

[9] E. Mathisen, (2011), "Security challenges and solutions in cloud computing," *Proc. IEEE International Conference on Digital Ecosystems and Technologies*, pp. 208–212.

[10] Cloud Security Alliance, (n.d.), "Guidance for critical areas of focus in cloud computing v3.0," [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf.

[11] Z. Shen and Q. Tong, (2010), "The security of cloud computing system enabled by trusted computing technology," *Proc. International Conference on Signal Processing Systems (ICSPS)*, pp. V2-11–V2-15.

[12] J. Feng, Y. Chen, D. Summerville, W. S. Ku, and Z. Su, (2011), "Enhancing cloud storage security against roll-back attacks with a new fair multiparty non-repudiation protocol," *Proc. IEEE International Conference on Cloud Networking and Computing (CNNC)*, pp. 521–522.

[13] J. Hamilton, (2009), "Cooperative expendable micro-slice servers (CEMS): Low cost, low power servers for Internet-scale services," *Proc. Conference on Innovative Data Systems Research (CIDR)*.

[14] D. Brooks et al., (2000), "Power-aware microarchitecture: Design and modeling challenges for next-generation microprocessors," *IEEE Micro*, Vol. 20, No. 6, pp. 26–44, Nov.–Dec.

[15] N. Vasic et al., (2009), "Making cluster applications energy-aware," *Proc. Automated Control for Data Centers and Clouds*.

[16] ETSI, (n.d.), "Cloud standardization," [Online]. Available: http://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf.